We claim:

1. A system for protecting keys used to digitally sign files to be downloaded to a terminal, comprising:

a smartcard having stored thereon a private key; and

a file signing tool arranged to receive a file to be signed, to access the smartcard, and to download signed files to the terminal,

wherein the smartcard includes an embedded secure processor programmed to perform all digital signing operations that require access to the private key.

2. A system as claimed in claim 1, wherein the smartcard also has stored thereon a signer certificate containing a public key corresponding to said private key.

3. A system as claimed in claim 2, wherein said file signer tool is arranged to retrieve said signer certificate from said smartcard and append the signer certificate to the signed file for use by the terminal in authenticating a digital signature generated by the smartcard and file signing tool.

4. A system as claimed in claim 3, wherein the signer certificate includes a field designating file types that may be authenticated by the signer certificate.

5. A system as claimed in claim 3, further comprising an owner certificate installed on said terminal for use by the terminal in authenticating the signer certificate.

6. A system as claimed in claim 1, wherein the smartcard also has stored thereon a PIN, and wherein said smartcard is arranged to perform digital signing operations only if a corresponding PIN is input through said file signing tool.

7. A system as claimed in claim 6, wherein said smartcard has stored thereon an authentication level indicating a number of PINs that must be input in order to access the smartcard.

8. A system as claimed in claim 7, wherein said PINs that must be input are combined by a logical exclusive OR operation in order to obtain a combined PIN to be compared with a PIN stored on the smartcard before said digital signing operations are performed.

9. A system as claimed in claim 7, wherein different ones of said PINs permit access to different private keys and public keys certificates having different file type properties, thereby enabling different authorization levels to be established.

10. A system for protecting keys used to digitally sign files to be downloaded to a terminal, comprising:

a smartcard; and

means for storing a private key on the smartcard and means for protecting the private key by requiring input of multiple PINs before the smartcard can be accessed,

wherein the smartcard includes an embedded secure processor programmed to perform all digital signing operations that require access to the private key.

11. A method of protecting keys used to digitally sign files to be downloaded to a terminal, comprising the steps of:

providing a smartcard having stored thereon a private key;

utilizing a secure processor embedded in the smartcard to perform all digital signing operations that require access to the private key.

12. A method as claimed in claim 11, further comprising the steps of storing the private key on the smart card and of requiring input of multiple PINs before granting access to functions performed by the smartcard.

13. A method as claimed in claim 11, further comprising the step of supplying a file to be signed to a file signing tool, using the file signing tool to access the smartcard, and downloading signed files to the terminal.

14. A method as claimed in claim 11, further comprising the step of storing on the smartcard a signer certificate containing a public key corresponding to said private key.

15. A method as claimed in claim 14, further comprising the step of using a file signer tool to retrieve the signer certificate from said smartcard and append the signer certificate to the signed file for use by the terminal in authenticating a digital signature generated by the smartcard and file signing tool.

16. A method as claimed in claim 15, further comprising the step of designating file types that may be

authenticated by the signer certificate, and including the file type designation in the signer certificate.

17. A method as claimed in claim 15, further comprising the step of authenticating the signer certificate by referring to an owner certificate pre-installed in said terminal.

18. A method as claimed in claim 11, wherein the smartcard also has stored thereon at least one PIN, and further comprising the step of causing the smartcard to perform digital signing operations only if a corresponding at least one PIN is input through a file signing tool.

19. A method as claimed in claim 18, further comprising the steps of:

storing an authentication level on the smartcard, said authentication level indicating a number of PINs that must be input in order to access the smartcard;

reading the authentication level and prompting at least one user to input said PINs;

combining said PINs to obtain a combined PIN; and

comparing said combined PIN with said at least one PIN stored on the smartcard before said digital signing operations are performed.

20. A method as claimed in claim 18, further comprising the step of storing on said smartcard a plurality of said PINs in order to permit access to different private keys and public keys certificates having different file type properties, thereby enabling different authorization levels to be established.